Microsoft Security Hands-On Lab
MS2811 - Applying Microsoft Security Guidance
One-Day, Instructor-Led, Hands-On Lab

This course is a one-day instructor-led, hands-on lab that allows students to apply information and guidance that can help in implementing and managing security in a network based on Microsoft® Windows®.

Audience
Attendees will be current IT professionals with experience using Microsoft Windows 2000 Server or Microsoft Windows Server™ 2003 and with knowledge of Active Directory® concepts. The students will be in an environment where they are responsible for aspects of security management and deployment associated with their internal network infrastructure and Internet or intranet services.

After completing this hands-on lab, students will be able to:

- Implement Group Policy.
- Create and work with user accounts and security groups.
- Implement account policies and security templates.
- Implement security for Web services.
- Monitor events and intruder detection.
- Manage software and security updates

Prerequisites
The target audience must have good baseline IT skills, because the concepts presented in these labs will build on their current experience.

Student Materials
The student kit includes a comprehensive workbook and other necessary materials for this class.


In this lab, attendees will perform hands-on exercises that cover key concepts necessary to increase security for Windows 2000 Server and Windows Server 2003.

Exercises
Exercise 1: Active Directory and Group Policy on Windows 2000
- Configuring Group Policy
- Configuring computer security policy settings
- Viewing account, user, and group properties
- Applying account policies
- Configuring IPSec
- Applying IPSec policies
- Deploying certificates for IPSec

Exercise 3: Implementing Web Service Security for IIS 5.0
- Implementing security for IIS 5.0 Web servers
- Streamlining the security configuration of Web servers

- New Active Directory features of Windows Server 2003
- Using the Server Role Wizard to establish a baseline
- Customizing configurations to support security requirements

Exercise 5: Implementing Web Service Security for IIS 6.0
- Maintaining and fine-tuning IIS 6.0 security

Exercise 6: Implementing Intrusion Detection and Event Monitoring
- Detecting network intrusions
- Performing event analysis
- Searching audit logs

Exercise 7: Implementing Remote Access and Virtual Private Networks (If Time Permits)
- Reviewing the quarantine features
- Editing an example start-up script

Lab 2: Implementing Client Security for Windows 2000 and Windows XP

In this lab, attendees will perform hands-on exercises that cover key technologies for managing the configuration of client security.

Exercises

Exercise 1: Securing Clients Using Group Policy
- Active Directory and Group Policy
- Configuring Group Policy

Exercise 2: Implementing Security Using Security Templates
- Applying security templates
- Implementing recommendations for mixed environments
Exercise 3: Implementing Shared Resource Security
- Managing shares and share security
- Implementing multi-user configurations

Exercise 4: Using PKI technologies on Client Computers
- Implementing encryption by using Encrypting File System (EFS)
- Backing up and restoring EFS keys
- Using Outlook Rights Management (RM) features

Exercise 5: Implementing Firewall Security
- Enabling Internet Connection Firewall (ICF)
- Customizing ICF ports

Exercise 6: Configuring Clients for Wireless Security (If Time Permits)
- Implementing security for wireless network access

Lab 3: Implementing Security for Windows Server System Applications

In this lab, attendees will perform hands-on exercises that introduce key security concepts for Windows Server System applications, such as Microsoft Exchange Server and Microsoft SQL Server™.

Exercises

Exercise 1: Configuring Microsoft SQL Server for Internet Security
- Protecting Database Servers
- 10 Steps to Making SQL Servers more secure

Exercise 2: Implementing Security for Microsoft Exchange Server
- Securing an Exchange Server
- 10 Steps to making Exchange Servers more secure

Exercise 3: Implementing Internet Access Security for Microsoft Exchange Server
- Securing Credentials with SSL
- Secure RPC

Lab 4: Managing Security Updates

In this lab, attendees will perform hands-on exercises that cover key patch management technologies, including Microsoft Baseline Security Analyzer (MBSA), Microsoft Software Update Services (SUS), and Microsoft Systems Management Server (SMS) 2003.
Exercises

Exercise 1: Implementing a Software Maintenance Infrastructure
- Managing software updates
- Slipstreaming service packs and hotfixes
- Analyzing software status by using MBSA
- Scripting MBSA using batch files and MBSAcli.exe
- Deploying service packs and hotfixes
- Creating media and scripts for mobile patch distribution

Exercise 2: Implementing Automated Updates with Microsoft Software Update Services
- Installing SUS (Description Only)
- Configuring SUS
- Manually deploying SUS client software
- Implementing policy-based deployment

Exercise 3: Implementing Automated Updates with SMS
- Installing multiple hotfixes in packages
- Deploying software and security updates by using SMS

Exercise 4: Checking the Deployment of Patches Using MBSA (If Time Permits)
- Analyzing patch status before deployment
- Analyzing patch status after deployment